EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	1	("6668322").PN.	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2007/09/10 11:03
S2	801	@ad<"20040223" and (certificate same (otp (one adj time) seed))	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2007/09/10 17:08
S3	361	@ad<"20040223" and (certificate same (otp (one adj time)))	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2007/09/10 11:04
S4	452	@ad<"20040223" and (certificate same (seed))	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2007/09/10 11:05
S5	91	@ad<"20040223" and (certificate same (seed)) and (seed with (password otp key))	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2007/09/10 13:34
S6	1	"20070033642".pn.	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2007/09/10 13:35
S7	1	"20070130472".pn.	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2007/09/10 13:35
S8	41	@ad<"20040223" and ((encrypt$3 sign$3 encipher$3 encod$3) near4 seed) with (public adj key)	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2007/09/10 15:38
S9	1	"20050188202".pn.	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2007/09/10 14:02
S10	1	"7181602".pn.	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2007/09/10 14:02
S11	1963	@ad<"20040223" and (((public adj key) pki) near4 certificat$3) and ((certificate attribute) same (secret seed (random adj number)))	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2007/09/10 15:50
S12	893	@ad<"20040223" and (((public adj key) pki) near4 certificat$3) and ((certificate attribute) near5 (secret seed (random adj number)))	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2007/09/10 15:50
S13	56	@ad<"20040223" and (((public adj key) pki) near4 certificat$3) and ((attribute) near5 (secret seed (random adj number)))	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2007/09/10 16:01
S14	1	"7113594".pn.	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2007/09/10 17:08

EAST Search History

S16	98	@ad<"20040223" and (richards.in. wasilewski.in.) and certificat$4 and (set adj top)	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2007/09/11 10:47
S17	89	@ad<"20040223" and (richards.in. wasilewski.in.) and certificate and (set adj top)	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2007/09/11 12:56
S18	73	@ad<"20040223" and (richards.in. wasilewski.in.) and (certificate same (key seed)) and (set adj top)	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2007/09/11 12:57
S19	0	@ad<"20040223" and (richards.in. wasilewski.in.) and (certificate same (seed)) and (set adj top)	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2007/09/11 12:57
S20	5	@ad<"20040223" and (richards.in. wasilewski.in.) and (certificate same (ATTRIBUTE)) and (set adj top)	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2007/09/11 12:59
S21	373	@ad<"20040223" and (certificat$4 adj (authority issu$3)) same ((seed) (secret adj key))	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2007/09/11 13:01
S22	157	@ad<"20040223" and (certificat$4 adj (authority issu$3)) same (certificate near7 ((seed) (secret adj key)))	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2007/09/11 13:01
S23	11	@ad<"20040223" and (certificat$4 adj (authority issu$3)) same (certificate near7 seed)	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2007/09/11 13:16
S25	269	(settlement and terminal).ti.	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2007/09/11 13:03
S29	2	cho.in. and settlement and starbridge	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/09/11 13:05
S30	11	@ad<"20040223" and ((certificate) same ((one adj time) onetime one-time)) and (seed same ((one adj time) onetime one-time))	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2007/09/11 13:55
S31	71	@ad<"20040223" and (((one adj time) onetime one-time) near3 password) same (hash$3 same time)	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2007/09/11 14:05
S32	3	@ad<"20040223" and (((one adj time) onetime one-time) near3 password) same (hash$3 same date)	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2007/09/11 14:06
S33	1	@ad<"20040223" and (((one adj time) onetime one-time) near3 password) same (hash$3 near4 password) same input$4	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2007/09/11 14:06

EAST Search History

S34	5	@ad<"20040223" and (((one adj time) onetime one-time) near3 password) same (hash$3 near4 password) same (input$4 enter$3)	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2007/09/11 14:08
S35	7	@ad<"20040223" and ((one adj time) onetime one-time) same (hash$3 with password with (secret date)) and (password same (input$4 enter$3))	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2007/09/11 14:16
S36	345	@ad<"20040223" and (user near4 password) and (password same hash$3 same (time counter date))	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2007/09/11 14:17
S37	15	@ad<"20040223" and (user near4 password) and (password same hash$3 same (time counter date) same replay$5)	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2007/09/11 15:42
S38	171	713/173.ccls.	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2007/09/11 15:42
S39	901	713/156.ccls.	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2007/09/11 15:43
S40	455	713/175.ccls.	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2007/09/11 15:44
S41	267	726/10.ccls.	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2007/09/11 15:45
S43	675	725/25.ccls.	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2007/09/11 15:45
S44	2191	S38 S39 S40 S41 S43	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2007/09/11 15:45
S45	26	S44 and (certificate) and (one adj time adj password)	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2007/09/11 15:51
S46	7	((NICOLAS) near2 (POPP)).INV.	USPAT	OR	ON	2007/09/11 15:46
S47	29	((NICOLAS) near2 (POPP)).INV.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/09/11 15:46
S48	3	S47 and certificate	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2007/09/11 15:51

Google

public key certificate seed attribute Search Advanced Search Preferences

New! View and manage your web history

Web Results **1 - 10** of about **592,000** for **public key certificate seed attribute**. (**0.07** seconds)

com.adobe.livecycle.signatures.client.types ...
Represents a **certificate seed** value dictionary. Before working with this class, it is recommended that .... The **key** can be any legal **attribute** identifier. ...
livedocs.adobe.com/.../com/adobe/livecycle/signatures/client/types/**CertificateSeed**ValueOptionSpec.html - 41k - Cached - Similar pages

draft-ietf-spki-cert-structure-00 - Simple **Public Key Certificate** ...
Simple **Public Key Certificate** Carl M. Ellison INTERNET-DRAFT CyberCash, Inc. Expires: 22 ..... These **attributes** are independent of **certificate** format. ...
tools.ietf.org/html/draft-ietf-spki-cert-structure-00 - 119k - Cached - Similar pages

internet x 509 **public key** infrastructure **certificate** and
Standards Track [Page 20] RFC 2459 Internet X.509 **Public Key** Infrastructure January 1999 (a) **attribute** values encoded in different types (e.g., ...
www.ietf.org/rfc/rfc2459.txt - 273k - Cached - Similar pages

WMRMLicGen.**Attribute**
The **public key** is included in the **certificate** ' sent to the license issuer by ... KeyID = sKeyID ' Use the **key** ID and your stored license **key seed** to create ...
msdn2.microsoft.com/en-us/library/bb614704.aspx - 15k - Cached - Similar pages

RFC 2459 (rfc2459) - Internet X.509 **Public Key** Infrastructure ...
RFC 2459 - Internet X.509 **Public Key** Infrastructure **Certificate** and CRL Profile. ... Standard sets of **attributes** have been defined in the X.500 series of ...
www.faqs.org/rfcs/rfc2459.html - 259k - Cached - Similar pages

The PKI page
This page contains links to various sites and documents related to **Public Key** Infrastructure (PKI) material, especially links **certificate** authorities (CAs).
www.pki-page.org/ - 99k - Cached - Similar pages

[PDF] LNCS 2836 - An Efficient **Public-Key** Framework
File Format: PDF/Adobe Acrobat
number of extension is j, the refreshing period is L, and the control **seed** is r. Definition 3. A **public-key certificate** CERT ...
www.springerlink.com/index/DX65Y49CLFJWL7BY.pdf - Similar pages

[PDF] Digital Signatures in the PDF Language
File Format: PDF/Adobe Acrobat - View as HTML
certificate which binds a simple user-provided identity to a **public key** generated ..... the **seed** value a preference or a requirement. **Attributes** that can be ...
www.adobe.com/devnet/acrobat/pdfs/DigitalSignaturesInPDF.pdf - Similar pages

Method and system for generating and verifying a **key** protection ...
The system according to claim 15, wherein said received **key** protection **certificate** includes private contextual **attributes**, **public** contextual **attributes**, ...
www.freepatentsonline.com/20030005317.html - 43k - Cached - Similar pages

[PDF] SUMMARY OF ANSI X9.44 **Public Key** Cryptography for the Financial ...

File Format: PDF/Adobe Acrobat - View as HTML
Generate a random bit string **seed** of length hLen. .... Security **Attributes**. 4.1 Security of Factoring Based **Public Key** Cryptography ...
csrc.nist.gov/encryption/kms/sum44.pdf - Similar pages

1 2 3 4 5 6 7 8 9 10 **Next**

---

public key certificate seed attribute Search

Search within results | Language Tools | Search Tips | Dissatisfied? Help us improve

---

Web Results **1** - **10** of about **253,000** for **pki certificate secret one time password**. (**0.20** seconds)

[PPT] ESnet **PKI One Time Password** Support
File Format: Microsoft Powerpoint - View as HTML
ESnet **PKI One Time Password** Support. Grid response to **One Time Password** Initiative ... Demonstrate improved **certificate** validation techniques ...
forge.ogf.org/.../doc12902;jsessionid=E68210997358D7BB2527366619DEE3CF - Similar pages

Token device that generates and displays **one-time passwords** and ...
These authentication methods include **one-time password**, challenge response, **PKI**, digital **certificate**, and/or biometric. The token may also perform such ...
www.freepatentsonline.com/20050015588.html - 33k - Cached - Similar pages

Single **one-time password** token with single PIN for access to ...
In a conventional **PKI** system, the **certificate** authority issues digital ... 2a illustrates **one** embodiment of a **one-time password** token and single personal ...
www.freepatentsonline.com/20070130463.html - 86k - Cached - Similar pages
[More results from www.freepatentsonline.com]

[PDF] PKOTP - **One time password** method using public key cryptography
File Format: PDF/Adobe Acrobat - View as HTML
This paper explains a **one time password** system using smartcards and ... places where **PKI** technology is massively applied and still needs to add **one** more ...
www.gv.psu.edu/foweb/pdf/ENG_RI2006_Ramanujam.pdf - Similar pages

AGIMO | Appendix B - E-authentication mechanisms
Each user has a hand-held hardware device that generates each **one-time password** based on **secret** information in the device which is known to a central server ...
www.agimo.gov.au/infrastructure/authentication/agaf_b/impguidegovt/volume2/appendix_b - 19k - Cached - Similar pages

::Secure Electronic Banking with Koçbank::
"We appreciate Kobil as a competent partner in both technologies: with **one time passwords** as well as with **certificate**-based solutions", says Hishem Md. ...
www.kobil.de/index.php?id=358&type=2&tx_ttnews%5Btt_news%5D=62&tx_ttnews%5BbackPid%5D=228... - 14k - Cached - Similar pages

[PDF] Secure Electronic Banking with the Koçbank
File Format: PDF/Adobe Acrobat - View as HTML
retail banking customers using the **one time password** solution (OTP) SecOVID ... as central administrative solution for the **certificate**-based **PKI** (public key ...
www.kobil.de/uploads/media/pressrelease-kocbank_1v08_20051004_uk.pdf - Similar pages

[PPT] FERMI SAV Results
File Format: Microsoft Powerpoint - View as HTML

Uses pkinit extensions to authenticate user via X509 **certificate**. Description cont'd. **One Time Passwords**. Integrated with MyProxy via FreeRADIUS interface ...
middleware.internet2.edu/**pki**06/proceedings/chan-pam.ppt - Similar pages

rfc 2511 internet x 509 **pki certificate** request
The salt value is appended to the shared **secret** and the **one** way function (owf) ... the requester indicates that the **PKI** should not publish the **certificate** ...
www.ietf.org/rfc/rfc2511.txt - 48k - Cached - Similar pages

Title Index
[Reserved for Network **Time** Protocol (NTP). See RFC 1305. ..... The EAP Protected **One-Time Password** Protocol (EAP-POTP) · The EAP-PSK Protocol: A Pre-Shared ...
dret.net/rfc-index/titles - Similar pages

1 2 3 4 5 6 7 8 9 10 **Next**

---

pki certificate secret one time passw Search

Search within results | Language Tools | Search Tips | Dissatisfied? Help us improve

---

Terms used: **certificate 'one time password' public** Found **82** of **210,707**

Sort results by: relevance
Display results: expanded form
Save results to a Binder
Search Tips
Open results in a new window

Try an Advanced Search
Try this search in The ACM Guide

Results 1 - 20 of 82 Result page: **1** 2 3 4 5 next

Relevance scale

1 A smartcard for authentication in WLANs

Marc Loutrel, Pascal Urien, Guy Pujolle
October 2003 **Proceedings of the 2003 IFIP/ACM Latin America conference on Towards a Latin American agenda for network research LANC '03**
Publisher: ACM Press
Full text available: pdf(333.05 KB) Additional Information: full citation, abstract, references, index terms

Wireless LANs based on the IEEE 802.11b standard have spread very quickly over the past few years. Nevertheless a lot of security issues remain and stop its deployment in corporations. One of the most important issues is the authentication of a terminal to an Access Point. We propose an interface to integrate the Extensible Authentication Protocol into smartcards and will show that smartcards could constitute the de-facto device for authentication in Wireless LAN as they are for GSM and will ...

Keywords: authentication, smartcard, wireless LANs

2 Public-key cryptography and password protocols

Shai Halevi, Hugo Krawczyk
August 1999 **ACM Transactions on Information and System Security (TISSEC)**, Volume 2 Issue 3
Publisher: ACM Press
Full text available: pdf(275.84 KB) Additional Information: full citation, abstract, references, citings, index terms, review

We study protocols for strong authentication and key exchange in asymmetric scenarios where the authentication server possesses ~a pair of private and public keys while the client has only a weak human-memorizable password as its authentication key. We present and analyze several simple password authentication protocols in this scenario, and show that the security of these protocols can be formally proven based on standard cryptographic assumptions. Remarkably, our analysis shows optimal re ...

Keywords: dictionary attacks, hand-held certificates, key exchange, passwords, public passwords, public-key protocols

3 Secure password-based authenticated key exchange for web services

Liang Fang, Samuel Meder, Olivier Chevassut, Frank Siebenlist
October 2004 **Proceedings of the 2004 workshop on Secure web service SWS '04**

Publisher: ACM Press

Full text available: pdf(395.64 KB) Additional Information: full citation, abstract, references, citings, index terms

This paper discusses an implementation of an authenticated key-exchange method rendered on message primitives defined in the WS-Trust and WS-SecureConversation specifications. This IEEE-specified cryptographic method (AuthA) is proven-secure for password-based authentication and key exchange, while the WS-Trust and WS-SecureConversation are emerging Web Services Security specifications that extend the WS-Security specification. A prototype of the presented protocol is integrated in the WS-Resour ...

Keywords: authenticated key exchange, password, security, web services

4 ID-based secret-key cryptography

Marc Joye, Sung-Ming Yen

October 1998 **ACM SIGOPS Operating Systems Review**, Volume 32 Issue 4

Publisher: ACM Press

Full text available: pdf(513.15 KB) Additional Information: full citation, abstract, citings, index terms

This paper introduces *ID-based secret-key cryptography,* in which secret keys are privately and uniquely binded to an identity. This enables to extend public-key cryptography features at the high throughput rate of secret-key cryptography. As applications, efficient login protocols, an enhanced version of Kerberos, and an ID-based MAC algorithm are presented.ID-based systems were initially developed in the context of public-key cryptography by removing the need of explicit public keys. The ...

Keywords: ID-based systems, Kerberos, MACs, authentication protocols, one-time passwords, secret-key cryptography

5 Crypto-based identifiers (CBIDs): Concepts and applications

Gabriel Montenegro, Claude Castelluccia

February 2004 **ACM Transactions on Information and System Security (TISSEC)**, Volume 7 Issue 1

Publisher: ACM Press

Full text available: pdf(262.76 KB) Additional Information: full citation, abstract, references, citings, index terms, review

This paper addresses the identifier ownership problem. It does so by using characteristics of Statistical Uniqueness and Cryptographic Verifiability (SUCV) of certain entities which this document calls SUCV Identifiers and Addresses, or, alternatively, Crypto-based Identifiers. Their characteristics allow them to severely limit certain classes of denial-of-service attacks and hijacking attacks. SUCV addresses are particularly applicable to solve the address ownership problem that hinders mechani ...

Keywords: Security, address ownership, authorization, group management, mobile IPv6, opportunistic encryption

6 Extending NCP for protocols using public keys

Aviel D. Rubin

December 1997 **Mobile Networks and Applications**, Volume 2 Issue 3

Publisher: Kluwer Academic Publishers

Full text available: pdf(635.20 KB) Additional Information: full citation, abstract, references, index terms

One of the greatest obstacles to wide-spread deployment of wireless mobile systems is

security. Cryptographically strong protocols and algorithms are required to enable secure communication over links that are easy to monitor and control by an attacker. While good cryptographic algorithms exist, it is difficult to design protocols that are immune to malicious attack. Good analysis techniques are lacking. This paper presents extensions to a technique for specifying and analyzing nonmonotonic ...

7 A heterogeneous-network aided public-key management scheme for mobile ad hoc networks

Yuh-Min Tseng
January 2007 **International Journal of Network Management**, Volume 17 Issue 1
Publisher: John Wiley & Sons, Inc.
Full text available: pdf(231.50 KB) Additional Information: full citation, abstract, references, index terms

A mobile ad hoc network does not require fixed infrastructure to construct connections among nodes. Due to the particular characteristics of mobile ad hoc networks, most existing secure protocols in wired networks do not meet the security requirements for mobile ad hoc networks. Most secure protocols in mobile ad hoc networks, such as secure routing, key agreement and secure group communication protocols, assume that all nodes must have pre-shared a secret, or pre-obtained public-key certificate ...

8 Staying secure in an insecure world: 802.1x secure wireless computer connectivity for students, faculty, and staff to the campus network

Steven K. Brawn, R. Mark Koan, Kelly Caye
October 2004 **Proceedings of the 32nd annual ACM SIGUCCS conference on User services SIGUCCS '04**
Publisher: ACM Press
Full text available: pdf(398.37 KB) Additional Information: full citation, abstract, references, index terms

During this past year, the ASU West IT Department has successfully implemented network connectivity throughout the campus for users who desire to use their computers in places other than the usual designated office spaces and computer labs. Students and staff alike can now access their network file shares, check email, browse the web, and work on projects while sitting in the cafeteria, out on the grass, or under the shade of a tree.

With the constant threat of virus attacks, Trojans, ...

Keywords: 802.1x, PEAP, VPN, authentication, dynamic WEP, wireless network

9 Columns: Surfing the net for software engineering notes

Mark Doernhoefer
March 2001 **ACM SIGSOFT Software Engineering Notes**, Volume 26 Issue 2
Publisher: ACM Press
Full text available: pdf(1.99 MB) Additional Information: full citation

10 On the efficient implementation of fair non-repudiation

Cheng-Hwee You, Jianying Zhou, Kwok-Yan Lam
October 1998 **ACM SIGCOMM Computer Communication Review**, Volume 28 Issue 5
Publisher: ACM Press
Full text available: pdf(689.48 KB) Additional Information: full citation, abstract, citings, index terms

Due to the explosive growth of electronic businesses carried on the Internet, non-repudiation services turn out to be increasingly important. Non-repudiation services protect the transacting parties against any false denial that a particular event or action has

taken place, in which evidence will be generated, collected and maintained to enable the settlement of disputes. Several fair non-repudiation protocols have been proposed, which support non-repudiation of origin and non-repudiation of rec ...

Keywords: dispute resolution, evidence chaining, fair non-repudiation, validity of evidence

11 A new family of authentication protocols

Ross Anderson, Francesco Bergadano, Bruno Crispo, Jong-Hyeon Lee, Charalampos Manifavas, Roger Needham

October 1998 **ACM SIGOPS Operating Systems Review**, Volume 32 Issue 4

Publisher: ACM Press

Full text available: pdf(821.42 KB) Additional Information: full citation, abstract, citings, index terms

We present a related family of authentication and digital signature protocols based on symmetric cryptographic primitives which perform substantially better than previous constructions. Previously, one-time digital signatures based on hash functions involved hundreds of hash function computations for each signature; we show that given online access to a timestamping service, we can sign messages using only two computations of a hash function. Previously, techniques to sign infinite streams invol ...

Keywords: authentication, hashing, non-repudiation, timestamping

12 Public-key cryptography and password protocols

Shai Halevi, Hugo Krawczyk

November 1998 **Proceedings of the 5th ACM conference on Computer and communications security CCS '98**

Publisher: ACM Press

Full text available: pdf(1.28 MB) Additional Information: full citation, references, citings, index terms

13 Unlinkable serial transactions: protocols and applications

Stuart G. Stubblebine, Paul F. Syverson, David M. Goldschlag

November 1999 **ACM Transactions on Information and System Security (TISSEC)**, Volume 2 Issue 4

Publisher: ACM Press

Full text available: pdf(184.87 KB) Additional Information: full citation, abstract, references, citings, index terms, review

We present a protocol for unlinkable serial transactions suitable for a variety of network-based subscription services. It is the first protocol to use cryptographic blinding to enable subscription services. The protocol prevents the service from tracking the behavior of its customers, while protecting the service vendor from abuse due to simultaneous or cloned use by a single subscriber. Our basic protocol structure and recovery protocol are robust against failure in protocol termination. ...

Keywords: anoymity, blinding, cryptographic protocols, unlinkable serial transactions

14 ISOC symposium on network and distributed systems security

Dan Nessett

April 1994 **ACM SIGCOMM Computer Communication Review**, Volume 24 Issue 2

Publisher: ACM Press

Full text available: Additional Information:

pdf(821.23 KB) full citation, index terms

15 Article abstracts with full text online: Globus security model for grid environment

Nitin V. Kanaskar, Umit Topaloglu, Coskun Bayrak
November 2005 **ACM SIGSOFT Software Engineering Notes**, Volume 30 Issue 6
Publisher: ACM Press
Full text available: pdf(372.40 KB) Additional Information: full citation, abstract, references, index terms

Grid technology is increasingly being looked upon as a natural extension of the internet for engaging in complex data processing tasks over resources which are distributed across the world. Architects and developers employing grid systems must take into consideration security implications. Dynamic generation of virtual organizations leads to a synergistic picture which has to address security requirements never encountered before. Globus toolkit has devised a framework for making secure use of g ...

16 Revokable and versatile electronic money (extended abstract)

Markus Jakobsson, Moti Yung
January 1996 **Proceedings of the 3rd ACM conference on Computer and communications security CCS '96**
Publisher: ACM Press
Full text available: pdf(1.53 MB) Additional Information: full citation, references, citings, index terms

17 Fair exchange with a semi-trusted third party (extended abstract)

Matthew K. Franklin, Michael K. Reiter
April 1997 **Proceedings of the 4th ACM conference on Computer and communications security CCS '97**
Publisher: ACM Press
Full text available: pdf(869.47 KB) Additional Information: full citation, references, citings, index terms

18 Securing the commercial Internet

Anish Bhimani
June 1996 **Communications of the ACM**, Volume 39 Issue 6
Publisher: ACM Press
Full text available: pdf(1.14 MB) Additional Information: full citation, references, citings, index terms, review

19 Pedagogy: A proposed curriculum of cryptography courses

Wasim A. Al-Hamdani, Ivory J. Griskell
September 2005 **Proceedings of the 2nd annual conference on Information security curriculum development InfoSecCD '05**
Publisher: ACM Press
Full text available: pdf(148.92 KB) Additional Information: full citation, abstract, references, index terms

The Cryptography Course is a major part of Computer security, Information security, Network security and all Information security related courses [12, chapter 1]. This course could be offered to undergraduate level (S level) or graduate level students. This article focuses on the problem:If the Cryptography course is offered as two consecutive courses, there is no problem because there are about 30-32 weeks of instruction for the 3-credit course (about 100 hours). This quantity of time is quite ...

Keywords: curriculum development, curriculum instruction, information assurance, information assurance curriculum, information security, information security curriculum

20 Mobile computing symposium: security and applications in mobile computing: A server-aided signature scheme for mobile commerce

Chin-Ling Chen, Chih-Cheng Chen, Ling-Chun Liu, Gwoboa Horng

August 2007 **Proceedings of the 2007 international conference on Wireless communications and mobile computing IWCMC '07**

Publisher: ACM Press

Full text available: pdf(318.30 KB) Additional Information: full citation, abstract, references, index terms

Mobile communications offer a wide variety of services to people. All mobile subscribers can use a mobile device to access various resources and conduct their business anytime from anywhere. This feature has contributed greatly to the rapid development of mobile commerce.

In fact, the Personal Trusted Device (PTD, such as PDA or mobile phone) lacks of computing resources has become a problem in mobile commerce development. In this paper, we overcome the limited computation power of mob ...

Keywords: hashing chain, mobile commerce, server-aided signature

Results 1 - 20 of 82 Result page: **1** 2 3 4 5 next

Terms used: **certificate 'one time password' public** Found **82** of **210,707**

Sort results by: relevance | Save results to a Binder | Try an Advanced Search

Display results: expanded form | Search Tips | Try this search in The ACM Guide

Open results in a new window

Results 21 - 40 of 82 Result page: previous 1 **2** 3 4 5 next

Relevance scale

21 On-line e-wallet system with decentralized credential keepers

Stig Frode Mjølsnes, Chunming Rong

February 2003 **Mobile Networks and Applications**, Volume 8 Issue 1

Publisher: Kluwer Academic Publishers

Full text available: pdf(240.23 KB) Additional Information: full citation, abstract, references, index terms

We propose a generalization of the architecture of an electronic wallet, as first developed in the seminal European research project CAFE. With this model you can leave most of the content of your electronic wallet at the security of your residential electronic keeper, while roaming with your favorite mobile terminals. Emerging mobile handsets with both short range Bluetooth and cellular GPRS communications provide a sufficient communication platform for this electronic wallet architecture. Howe ...

Keywords: digital credentials, e-wallet architecture, mobile commerce, payment protocols, privacy

22 DRM experience: Analysis of security vulnerabilities in the movie production and distribution process

Simon Byers, Lorrie Cranor, Dave Korman, Patrick McDaniel, Eric Cronin

October 2003 **Proceedings of the 3rd ACM workshop on Digital rights management DRM '03**

Publisher: ACM Press

Full text available: pdf(285.80 KB) Additional Information: full citation, abstract, references, citings, index terms, review

Unauthorized copying of movies is a major concern for the motion picture industry. While unauthorized copies of movies have been distributed via portable physical media for some time, low-cost, high-bandwidth Internet connections and peer-to-peer file sharing networks provide highly efficient distribution media. Many movies are showing up on file sharing networks shortly after, and in some cases prior to, theatrical release. It has been argued that the availability of unauthorized copies directl ...

Keywords: digital rights management, file sharing, insider attacks, multimedia, physical security, policy

23 Internet security: firewalls and beyond

Rolf Oppliger
May 1997 **Communications of the ACM**, Volume 40 Issue 5
Publisher: ACM Press
Full text available: pdf(339.15 KB) Additional Information: full citation, references, citings, index terms, review

24 Security protocols: Provably secure password-based authentication in TLS
Michel Abdalla, Emmanuel Bresson, Olivier Chevassut, Bodo Möller, David Pointcheval
March 2006 **Proceedings of the 2006 ACM Symposium on Information, computer and communications security ASIACCS '06**
Publisher: ACM Press
Full text available: pdf(378.65 KB) Additional Information: full citation, abstract, references, index terms

In this paper, we show how to design an efficient, provably secure password-based authenticated key exchange mechanism specifically for the TLS (Transport Layer Security) protocol. The goal is to provide a technique that allows users to employ (short) passwords to securely identify themselves to servers. As our main contribution, we describe a new password-based technique for user authentication in TLS, called *Simple Open Key Exchange* (SOKE). Loosely speaking, the SOKE ciphersuites are un ...

Keywords: TLS, encrypted key exchange, password authentication

25 Protecting applications with transient authentication
Mark D. Corner, Brian D. Noble
May 2003 **Proceedings of the 1st international conference on Mobile systems, applications and services MobiSys '03**
Publisher: ACM Press
Full text available: pdf(294.40 KB) Additional Information: full citation, abstract, references, cited by

How does a machine know who is using it? Current systems authenticate their users infrequently, and assume the user's identity does not change. Such *persistent authentication* is inappropriate for mobile and ubiquitous systems, where associations between people and devices are fluid and unpredictable. We solve this problem with *Transient Authentication*, in which a small hardware token continuously authenticates the user's presence over a short-range, wireless link. We present the fo ...

26 New phase 1 exchange mode for IKE framework
J. M. Sierra, S. J. Shepherd
October 2000 **ACM SIGOPS Operating Systems Review**, Volume 34 Issue 4
Publisher: ACM Press
Full text available: pdf(441.58 KB) Additional Information: full citation, abstract, references

This paper describes some new extensions to the IKE Exchange Mode framework which both simplify the protocol and make each stage of the protocol more efficient. This will allow considerably faster security associations to be accomplished which is critical to system performance in time-limited protocols.

Keywords: IKE, ISAKMP, Internet Security, Security Protocols

27 Identity verification (authentication) working group
Tom Berson, P. Capek, J. Schweitzer, C. Weissman
April 1988 **ACM SIGSAC Review**, Volume 6 Issue 1
Publisher: ACM Press

Full text available: pdf(803.95 KB) Additional Information: full citation, abstract, index terms

Every reader of this report has at some time verified his or her identity to a computer system. Entry of a userid and password in response to computer prompting is the almost universal model for this simple but essential act.

28 SPINS: security protocols for sensor networks

Adrian Perrig, Robert Szewczyk, J. D. Tygar, Victor Wen, David E. Culler
September 2002 **Wireless Networks**, Volume 8 Issue 5

Publisher: Kluwer Academic Publishers

Full text available: pdf(213.37 KB) Additional Information: full citation, abstract, references, citings, index terms

Wireless sensor networks will be widely deployed in the near future. While much research has focused on making these networks feasible and useful, security has received little attention. We present a suite of security protocols optimized for sensor networks: SPINS. SPINS has two secure building blocks: SNEP and μTESLA. SNEP includes: data confidentiality, two-party data authentication, and evidence of data freshness. μTESLA provides authenticated broadcast for severely resource-constrained ...

Keywords: MANET, authentication of wireless communication, cryptography, mobile ad hoc networks, secrecy and confidentiality, secure communication protocols, sensor networks

29 Secure routing in ad hoc networks: Securing quality-of-service route discovery in on-demand routing for ad hoc networks

Yih-Chun Hu, David B. Johnson
October 2004 **Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks SASN '04**

Publisher: ACM Press

Full text available: pdf(218.91 KB) Additional Information: full citation, abstract, references, citings, index terms

An ad hoc network is a collection of computers (nodes) that cooperate to forward packets for each other over a multihop wireless network. Users of such networks may wish to use demanding applications such as videoconferencing, Voice over IP, and streaming media when they are connected through an ad~hoc network. Because overprovisioning, a common technique in wired networks, is often impractical in wireless networks for reasons such as power, cost, and government regulation, Quality of Service ...

Keywords: QoS routing, SQoS, ad hoc networks, quality-of-service, security, simulations

30 Response to "Problems with DCE security services"

Walter Tuvell
April 1996 **ACM SIGCOMM Computer Communication Review**, Volume 26 Issue 2

Publisher: ACM Press

Full text available: pdf(1.01 MB) Additional Information: full citation, index terms

31 Security architecture: Single sign-on for java web start applications using myproxy

Terry Fleury, Jim Basney, Von Welch
November 2006 **Proceedings of the 3rd ACM workshop on Secure web services SWS '06**

Publisher: ACM Press

Full text available: pdf(680.33 KB) Additional Information: full citation, abstract, references, index terms

Single sign-on is critical for the usability of distributed systems. While there are several authentication mechanisms which support single sign-on (e.g. Kerberos and X.509), it may be difficult to modify a particular legacy application to utilize an authentication scheme other than username/password. Asimple solution for single sign-on involves transmitting a user's password over the network. However, it is undesirable to expose a user's private password in an insecure environment. This paper d ...

Keywords: grid portals, session passwords, single sign-on

32 Protection and the control of information sharing in multics

Jerome H. Saltzer
July 1974 **Communications of the ACM**, Volume 17 Issue 7
Publisher: ACM Press

Full text available: pdf(1.75 MB) Additional Information: full citation, abstract, references, citings, index terms

The design of mechanisms to control the sharing of information in the Multics system is described. Five design principles help provide insight into the tradeoffs among different possible designs. The key mechanisms described include access control lists, hierarchical control of access specifications, identification and authentication of users, and primary memory protection. The paper ends with a discussion of several known weaknesses in the current protection mechanism design.

Keywords: Multics, access control, authentication, computer utilities, descriptors, privacy, proprietary programs, protected subsystems, protection, security, time-sharing systems, virtual memory

33 Pedagogy: eCommerce security

Bob Gehling, David Stankard
September 2005 **Proceedings of the 2nd annual conference on Information security curriculum development InfoSecCD '05**
Publisher: ACM Press
Full text available: pdf(95.37 KB) Additional Information: full citation, abstract, references, index terms

Internet security has become a consistent and growing problem as new Internet-based technologies and applications are developed. The number of security violation related incidents continues to increase [6]. A reported incident can be as simple as a single computer being compromised or as severe as a complete network compromise involving hundreds of client computers. All Internet content you read, send, and receive carries a risk. The amount of security risks increases at the same time that depen ...

Keywords: eCommerce, security, security awareness

34 Applications I: Secure fingerprint-based authentication for Lotus Notes®

Nalini K. Ratha, Jonathan H. Connell, Ruud M. Bolle
October 2001 **Proceedings of the 2001 workshop on Multimedia and security: new challenges MM&Sec '01**
Publisher: ACM Press
Full text available: pdf(731.41 KB) Additional Information: full citation, abstract, references

Fingerprints have been used to recognize people for several decades. The advent of low cost inkless fingerprint scanners coupled with extra compute power available in client workstations, biometrics in general and fingerprints in particular are being considered for

many secure authentication applications. Lotus Notes is a groupware supporting email access and other activities such as calendar management included in it. In this paper, we describe the architecture of a system that integrates bo ...

35 Problems with DCE security services

Gregory White, Udo Pooch
October 1995 **ACM SIGCOMM Computer Communication Review**, Volume 25 Issue 5
Publisher: ACM Press
Full text available: pdf(479.39 KB) Additional Information: full citation, abstract, index terms

Distributed computing is receiving an ever increasing amount of interest and with it come many challenges, not the least of which is how to maintain system and network security. Issues relating to user authentication, access authorization, and communication security must be addressed when multiple, heterogeneous systems are connected. While these issues have been addressed in OSFs DCE, several problems remain. This paper describes some of these problems.

36 LiSP: A lightweight security protocol for wireless sensor networks

Taejoon Park, Kang G. Shin
August 2004 **ACM Transactions on Embedded Computing Systems (TECS)**, Volume 3 Issue 3
Publisher: ACM Press
Full text available: pdf(487.54 KB) Additional Information: full citation, abstract, references, citings, index terms

Small low-cost sensor devices with limited resources are being used widely to build a self-organizing wireless network for various applications, such as situation monitoring and asset surveillance. Making such a sensor network secure is crucial to their intended applications, yet challenging due to the severe resource constraints in each sensor device. We present a *lightweight security protocol* (LiSP) that makes a tradeoff between security and resource consumption via efficient rekeying. ...

Keywords: Authentication, key management, lightweight security, sensor networks

37 A laboratory-based course on internet security

Prabhaker Mateti
January 2003 **ACM SIGCSE Bulletin , Proceedings of the 34th SIGCSE technical symposium on Computer science education SIGCSE '03**, Volume 35 Issue 1
Publisher: ACM Press
Full text available: pdf(138.18 KB) Additional Information: full citation, abstract, references, citings, index terms

We developed a laboratory-based course on Internet Security. The course is aimed at the senior undergraduate. This paper discusses the course and explains how others can set up their own labs to teach this course. All the laboratory work is conducted in a laboratory of PCs running Linux. We developed lecture notes for the course, and a web site to widely disseminate these materials.

Keywords: TCP/IP exploits, buffer overflow, ethics, firewalls, internet security, network security

38 Quality of security service

Cynthia Irvine, Timothy Levin
February 2001 **Proceedings of the 2000 workshop on New security paradigms NSPW '00**

Publisher: ACM Press
Full text available: pdf(684.54 KB) Additional Information: full citation, references, citings, index terms

Keywords: quality of security service, quality of service, security range, variant security

39 Long papers: Spy-resistant keyboard: more secure password entry on public touch screen displays
Desney S. Tan, Pedram Keyani, Mary Czerwinski
November 2005 **Proceedings of the 19th conference of the computer-human interaction special interest group (CHISIG) of Australia on Computer-human interaction: citizens online: considerations for today and the future OZCHI '05**
Publisher: Computer-Human Interaction Special Interest Group (CHISIG) of Australia
Full text available: pdf(454.44 KB) Additional Information: full citation, abstract, references

Current software interfaces for entering text on touch screen devices mimic existing mechanisms such as keyboard typing or handwriting. These techniques are poor for entering private text such as passwords since they allow observers to decipher what has been typed simply by looking over the typist's shoulder, an activity known as shoulder surfing. In this paper, we outline a general approach for designing security-sensitive onscreen virtual keyboards that allow users to enter private text withou ...

Keywords: input technique, keyboard, password, selective attention, touch screen, visual search

40 Securing a global village and its resources: baseline security for interconnected signaling system #7 telecommunications networks
Hank M. Kluepfel
December 1993 **Proceedings of the 1st ACM conference on Computer and communications security CCS '93**
Publisher: ACM Press
Full text available: pdf(1.19 MB) Additional Information: full citation, abstract, references, index terms

The resulting national focus on Network Integrity issues, spawned the development of an industry commitment to affect and realize a minimum security baseline for interconnected SS7 networks. In addition the affected carriers in those outage have accelerated their pursuit of secure solutions to today's intelligent networking.[2]This paper will focus on the development of the baseline and the current effort to take the baseline into national, e.g., National Ins ...

Results for "**(certificate <and> 'one time password' <and> public) <in> metadata**"

e-mail

Your search matched **0** of **1641691** documents.

A maximum of **100** results are displayed, **25** to a page, sorted by **Relevance** in **Descending** order.

Login

Username

Password

» Forgot your password?

Please remember to log out when you have finished your session.

No results were found.

Please edit your search criteria and try again. Refer to the Help pages if you need assistance revising your search

» Key

	Indicates full text access
IEEE JNL	IEEE Journal or Magazine
IET JNL	IET Journal or Magazine
IEEE CNF	IEEE Conference Proceeding
IET CNF	IET Conference Proceeding
IEEE STD	IEEE Standard